PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-006662
(43)Date of publication of application : 10.01.1997

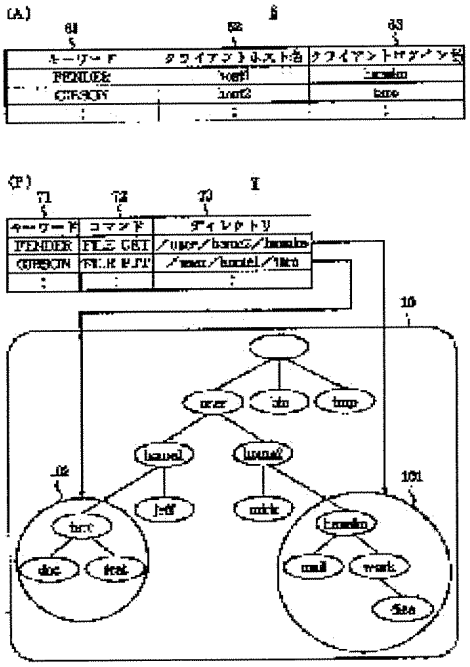
(51)Int.Cl. G06F 12/00
G06F 12/00
G06F 12/14
G06F 13/00
G06F 13/00

(21)Application number : 07-149214
(22)Date of filing : 15.06.1995

(71)Applicant : NEC CORP
(72)Inventor : HACHINOHE TOSHIHISA

(54) DEVICE AND METHOD FOR TRANSFERRING FILE

(57)Abstract:
PURPOSE: To prevent the wrong access and to improve the security by defining and limiting the directories of the accessible server file systems for every client.
CONSTITUTION: A server EW has a security management data base 6 which stores a key word 61, a client host name 62 that is defined by the word 61 and a login name 63, and an access definition data base 7 which sets an accessible range of every client by a key word 71, an execution command 72 that is defined by the word 71 and a directory 73. When a user file is transferred, the server EW designates a key word. Then the server EW collates the key word with the data base 7 in the file transfer state and carries out the command 72 in a designated directory.



LEGAL STATUS

[Date of request for examination] 15.06.1995
[Date of sending the examiner's decision of rejection] 17.02.1998
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－6662

(43)公開日　平成９年(1997)１月10日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	12/00	５３７	7623－5B	Ｇ０６Ｆ	12/00	５３７Ａ
		５４５	7623－5B			５４５Ｍ
	12/14	３１０			12/14	３１０Ｋ
	13/00	３５１	7368－5E		13/00	３５１Ｅ
		３５７	7368－5E			３５７Ｚ

審査請求　有　請求項の数４　ＯＬ　（全７頁）

(21)出願番号　特願平7－149214

(22)出願日　平成７年(1995)６月15日

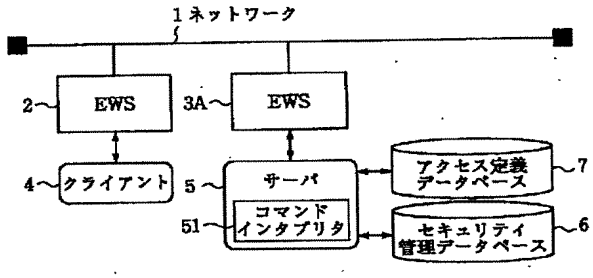
(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　八戸　理央
東京都港区芝五丁目７番１号　日本電気株式会社内

(74)代理人　弁理士　京本　直樹　（外２名）

(54)【発明の名称】　ファイル転送装置およびファイル転送方法

(57)【要約】
【目的】クライアント毎にアクセス可能なサーバファイルシステムのディレクトリの定義／制限を行い不正アクセスの防止及びセキュリティを向上させる。
【構成】サーバＥＷＳ３Ａが、キーワード６１とこのキーワード６１で定義するクライアントホスト名７１，ログイン名６３を格納したセキュリティ管理データベース６と、キーワード７１とこのキーワード７１で定義する実行コマンド７２，ディレクトリ７３とによりクライアント４の各々毎のアクセス可能範囲を設定するアクセス定義データベース７とを備える。ユーザのファイル転送時にキーワードを指定し（ステップＳ１）、サーバ５はファイル転送時にキーワードとアクセス定義データベース７を照合し（ステップＳ４）、定義されたディレクトリ内で（ステップＳ７）定義されたコマンド７２を実行する（ステップ１Ｓ）。



1

【特許請求の範囲】

【請求項１】　各々ネットワークを介して接続されユーザが使用するクライアントプログラムを走らせるクライアントＥＷＳとプログラムの解析ルーチンであるインタプリタを含むサーバプログラムを走らせるサーバＥＷＳとを備えるファイル転送装置において、

前記サーバＥＷＳが、キーワードとこのキーワードで定義するセキュリティ管理情報を格納したセキュリティ管理データベースと、

前記キーワードとこのキーワードで定義するアクセス定義情報により前記クライアントプログラムの各々毎のアクセス可能範囲を設定するアクセス定義データベースとを備えることを特徴とするファイル転送装置。

【請求項２】　前記セキュリティ管理情報が、前記キーワードの指定時に一組として定義する前記サーバプログラムへのアクセス許可対象のクライアントホスト名およびクライアントログイン名を含み、

前記アクセス定義情報が、前記キーワードの指定に対応して実行されるコマンドと、このコマンドの実行時にアクセス可能なディレクトリとを含むことを特徴とする請求項１記載のファイル転送装置。

【請求項３】　各々ネットワークを介して接続されユーザが使用するクライアントプログラムを走らせるクライアントＥＷＳとプログラムの解析ルーチンであるインタプリタを含むサーバプログラムを走らせるサーバＥＷＳとの間のファイル転送方法において、

前記サーバプログラムが、セキュリティ管理情報を格納したセキュリティ管理データベースと前記クライアントプログラムの各々毎のアクセス可能範囲を設定するアクセス定義データベースとを含み、

前記ユーザが前記クライアントプログラムを起動し第１のキーワードおよび転送ファイル名を入力するとともにこのクライアントプログラムが第１のクライアントホストおよびユーザ名を付加して前記サーバプログラムに送信する第１のステップと、

前記サーバプログラムが受信した第１のキーワードとクライアントホスト名とユーザ名の各々と前記セキュリティ管理データベースの第２のキーワードとクライアントホスト名とユーザ名の各々とを照合する第２のステップと、

前記照合の結果正式の登録クライアントであることを確認した場合に前記第１のキーワード対応の前記アクセス定義データベースの定義内容とを比較する第３のステップと、

前記第３のステップで前記第１のキーワードが正しいキーワードであることの確認後定義されたディレクトリを指定ディレクトリ以下以外へのアクセスを制限する仮想ルートディレクトリに置換する第４のステップと、

前記仮想ルートディレクトリ以下で転送対象ファイルを検索する第５のステップと、

2

前記転送ファイルを発見したとき前記アクセス定義データベース内でキーワードに対して一意に定義される転送コマンドを実行する第６のステップとを含むことを特徴とするファイル転送方法。

【請求項４】　前記第３のステップで前記第１のキーワードが正しいキーワードであることの確認後前記サーバプログラムが前記コマンドインタプリタを起動しこのコマンドインタプリタのプロンプトを前記クライアントプログラムに表示する第７のステップと、

前記ユーザが前記クライアントプログラムへの前記プロンプトの表示に応答して転送コマンドと転送対象のファイル名とを入力する第８のステップと、

前記第６のステップのファイル転送終了後他に転送対象ファイルの有無を確認し無ければ処理を終了し、有れば前記第７のステップへ戻り以降の処理を反復する第９のステップとをさらに含むことを特徴とする請求項３記載のファイル転送方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はファイル転送方法およびファイル転送装置に関し、特にコンピュータネットワークを介したコンピュータ間のファイル転送を行う場合のセキュリテイ機能を有するファイル転送方法およびファイル転送装置に関する。

【０００２】

【従来の技術】この種のコンピュータネットワークでは、ネットワーク上にさまざまな機能・サービスなどの資源を提供するサーバとユーザである複数のクランイアントとが存在し、クランイアントはサーバのハードディスク上に置いたプログラムファイルやデータファイルなどの上記資源を同時にアクセスして同時に実行したり更新をかけたりできるいわゆるファイル共有機能を有する。

【０００３】このファイル共有機能では、クライアントが目的と直接関係のないデータのコピーや悪用あるいは破壊することなどの不都合を防止するため、この種のアクセスを制限するためのセキュリテイ機能を有する。

【０００４】従来のこの種のセキュリテイ機能を有する一般的なファイル転送装置としてｆｔｐがある。

【０００５】従来の第１のファイル転送装置であるｆｔｐの構成をブロックで示す図５を参照すると、この従来の第１のファイル転送装置は、ネットワーク１により接続されたクライアント用のＥＷＳ２およびサーバ用のＥＷＳ３と、ＥＷＳ２上に存在するｆｔｐクライアントのプログラム（以下クライアント）４０と、ＥＷＳ３上に存在するコマンドインタプリタ部５１を含むｆｔｐサーバのプログラム（以下サーバ）５０と、ＥＷＳ３上に存在しクライアントユーザの認証を行うパスワード情報データベース８とを備える。

【０００６】パスワード情報データベース８の構成例を

示す図６を参照すると、このパスワード情報データベース８はユーザの登録名すなわちログイン名８１とパスワード文字８２との情報とを含む。

【０００７】次に、図５，６およびｆｔｐをバッチ方式で実行してファイル転送を行う従来の第１のファイル転送方法をフローチャートで示す図７を参照して、この従来の第１のファイル転送方法について説明すると、まずクライアント４０を起動し、ユーザ名，パスワード，ファイル名を入力する（ステップＰ１）。ｆｔｐサーバ５０はパスワード情報データベース８上のユーザ名，パスワード文字列とクライアントＥＷＳ２から通知されたユーザ名，パスワード文字列とを比較し（ステップＰ２）、比較結果（ステップＰ３）認証に失敗した場合はクライアント４０ににエラーを通知し（ステップＰ４）ファイル転送を行うことなく処理を終了する（ステップＰ１２，Ｐ１３）。認証に成功すると、サーバ５０では入力されたファイル名対応のファイルをサーバ４０の保有するファイルシステム内において検索し（ステップＰ７）、発見出来なければ（ステップＰ８）クライアント４０へエラーを通知、発見すればそのファイルの転送を開始する（ステップＰ９，Ｐ１０）。転送完了後、クライアント４０側、サーバ５０側の両プログラム共終了する（ステップ７１０，７１１）。

【０００８】次に、ｆｔｐをインタラクティブ方式で実行してファイル転送を行う従来の第２のファイル転送方法を図７と共通の処理は共通の文字／数字を付して同様にフローチャートで示す図８を参照すると、この従来の第２のファイル転送方法の第１のファイル転送方法との相違点は、ステップＰ３で認証に成功すると、サーバはコマンドインタプリタ５１を起動し、コマンドインタプリタ５１のプロンプトをクライアントへ表示するステップＰ５と、ユーザはクライアント４０に表示されたプロンプトから転送コマンドと転送対象のファイル名とを入力するステップＰ６と、さらに、ステップＰ９，Ｐ１０のファイル転送終了後、他に転送対象ファイルの有無を確認し無ければステップＰ１２で終了し、有ればステップＰ６へ戻り以下Ｐ１１までを反復するステップＰ１１とを付加することである。

【０００９】ｆｔｐで他のユーザからのアクセスを拒否するには、全てのディレクトリファイルに所有権を付加し、ステップＰ７の時点でエラーを発生し、ファイル自体のアクセスを拒否する必要がある。

【００１０】このように、サーバ５０はＥＷＳ３への接続時にのみユーザであるクライアント認証を行い、この接続完了後は基本的にクライアントはファイルシステムの全てを参照することが可能であり、上記接続後のクライアントのコマンド実行毎アクセス可能ディレクトリ空間のチェック機能を有しない。またクライアントの認証はパスワード情報データベース８を用いて行うが、このパスワード情報データベース８のログイン名はログイン

時のディレクトリを指定するだけでアクセス制限機能はなく、クライアント毎のディレクトリアクセス制限を行うことが出来ない。

【００１１】また、アクセス制限を行う従来の第２のファイル転送装置として、簡易版ｆｔｐ（ｔｆｔｐ）がある。この従来の第２のファイル転送装置ではユーザがアクセス可能なディレクトリを設定し、そのディレクトリより上位のディレクトリにはアクセス不可とすることが出来る。この設定は全ユーザに等しく有効となる。

【００１２】

【発明が解決しようとする課題】上述した従来の第１，第２のファイル転送方法および第１のファイル転送装置は、サーバプログラムがサーバマシンへの接続時にのみユーザであるクライアント認証を行い、この接続完了後は基本的にファイルシステムの全てを参照することが可能であり、上記接続後のユーザのアクセス可能ディレクトリ空間のチェック機能を有せず、またクライアントの認証を行うパスワード情報データベースのログイン名はログイン時のディレクトリの指定機能だけでアクセス制限機能はないので、同一ファイルシステム内の異なったディレクトリ空間に異なるユーザがそれぞれファイルを所有している場合、他人の管理するディレクトリ空間にアクセス可能であるため、ユーザ間での機密保持が出来ないという欠点があった。

【００１３】また、ディレクトリやファイルの所有権定義により相互排除を設定することは可能ではあるが、全てのディレクトリやファイルの一つ一つに対して矛盾なく設定するのは非常に困難であるという問題点があった。

【００１４】また、従来の第２のファイル転送装置は、ディレクトリアクセス制限機能を有するが、ユーザの認証を行わないため、アクセス制限をクライアント／ユーザ単位で行うことが出来ず、異なるクライアント／ユーザ間のサーバ上でのデータのアクセス制限を行えないというという欠点があった。

【００１５】

【課題を解決するための手段】本発明のファイル転送装置は、各々ネットワークを介して接続されユーザが使用するクライアントプログラムを走らせるクライアントＥＷＳとプログラムの解析ルーチンであるインタプリタを含むサーバプログラムを走らせるサーバＥＷＳとを備えるファイル転送装置において、前記サーバＥＷＳが、キーワードとこのキーワードで定義するセキュリティ管理情報を格納したセキュリティ管理データベースと、前記キーワードとこのキーワードで定義するアクセス定義情報により前記クライアントプログラムの各々毎のアクセス可能範囲を設定するアクセス定義データベースとを備えて構成されている。

【００１６】本発明のファイル転送方法は、各々ネットワークを介して接続されユーザが使用するクライアント

プログラムを走らせるクライアントＥＷＳとプログラムの解析ルーチンであるインタプリタを含むサーバプログラムを走らせるサーバＥＷＳとの間のファイル転送方法において、前記サーバプログラムが、セキュリティ管理情報を格納したセキュリティ管理データベースと前記クライアントプログラムの各々毎のアクセス可能範囲を設定するアクセス定義データベースとを含み、前記ユーザが前記クライアントプログラムを起動し第１のキーワードおよび転送ファイル名を入力するとともにこのクライアントプログラムが第１のクライアントホストおよびユーザ名を付加して前記サーバプログラムに送信する第１のステップと、前記サーバプログラムが受信した第１のキーワードとクライアントホスト名とユーザ名の各々と前記セキュリティ管理データベースの第２のキーワードとクライアントホスト名とユーザ名の各々とを照合する第２のステップと、前記照合の結果正式の登録クライアントであることを確認した場合に前記第１のキーワード対応の前記アクセス定義データベースの定義内容とを比較する第３のステップと、前記第３のステップで前記第１のキーワードが正しいキーワードであることの確認後定義されたディレクトリを指定ディレクトリ以下以外へのアクセスを制限する仮想ルートディレクトリに置換する第４のステップと、前記仮想ルートディレクトリ以下で転送対象ファイルを検索する第５のステップと、前記転送ファイルを発見したとき前記アクセス定義データベース内でキーワードに対して一意に定義される転送コマンドを実行する第６のステップとを含むことを特徴とするものである。

【００１７】

【実施例】次に、本発明の第１の実施例を図５と共通の構成要素には共通の参照文字／数字を付して同様にブロックで示す図１を参照すると、この図に示す本実施例のファイル転送装置は、従来と共通のネットワーク１と、クライアントプログラム（以下クライアント）４とを含むクライアント用のＥＷＳ２とに加えて、ネットワーク１に接続したサーバ用のＥＷＳ３Ａと、ＥＷＳ３Ａ上に走らせるコマンド解析ルーチン（インタプリタ）５１を含むサーバプログラム（以下サーバ）５と、セキュリティ管理のためのセキュリティ管理データベース６と、クライアント毎のアクセス可能範囲を定義するアクセス定義データベース７とを備える。

【００１８】セキュリティ管理データベース６の内容を示す図２（Ａ）を参照すると、このセキュリティ管理データベース６は、キーワード６１と、そのキーワードの指定時に一組として定義するサーバ３Ａへのアクセス許可対象のクライアントホスト名６２およびクライアントログイン名６３を含む。サーバ５はクライアント４より送信されてきたキーワード，クライアントホスト名，クライアントユーザ名の各々をこのセキュリティ管理データベース６のこれら内容６１～６３と照合し、正しく登録されていなければアクセス要求を拒絶する。

【００１９】ＥＷＳ３Ａ上に置かれたアクセス定義データベース７の内容およびキーワードにより限定されるアクセス範囲を示す図２（Ｂ）を参照すると、アクセス定義データベース７は一組として定義するキーワード７１と、そのキーワードの指定時に実際に実行されるコマンド７２と、コマンド７２の実行時にアクセス可能なディレクトリ７３とを含む。この図において、全体のファイルシステム１０に対して、キーワード７１「ＦＥＮＤＥＲ」を指定した場合のアクセス可能なディレクトリ範囲１０１と、キーワード７１「ＧＩＢＳＯＮ」を指定した場合にアクセス可能なディレクトリ範囲１０２とをそれぞれ示す。

【００２０】次に、図１，２，および本実施例のファイル転送装置をバッチ方式に適用した場合の本発明の第２の実施例のファイル転送方法の処理をフローチャートで示す図３を参照して本実施例の動作について説明すると、まず、ユーザはクライアントプログラム４を起動しキーワード，転送ファイル名を入力する（ステップＳ１）。サーバ５へは入力キーワード，転送ファイル名の他、クライアント４が自動的にクライアントホスト名，ユーザ名を取得し、これらの情報がサーバ５に送信される。サーバ５は受信したキーワード，クライアントホスト名，ユーザ名の各々とセキュリティ管理データベース６の内容６１～６３とを照合する（ステップＳ２）。照合の結果（ステップＳ３）、正式に登録されたクライアントであることが確認出来なかった場合、クライアント４にエラー通知を行い（ステップＳ４）、ファイル転送を行うことなく処理を終了する（ステップＳ１５，Ｓ１６）。確認出来た場合、通知されたキーワードとアクセス定義データベースの定義内容とを比較し（ステップＳ７）、正しいキーワードであることを確認した後（ステップＳ８）定義されたディレクトリを仮想的にルートディレクトリに置き換える（ステップＳ９）。このステップＳ９によって、指定したディレクトリ以下以外へのアクセスを制限する。次に指定したディレクトリ（仮想ルートディレクトリ）以下で転送ファイルを検索し（ステップＳ１０）、ファイルが発見されれば（ステップＳ１１）アクセス定義データベース７内でキーワードに対して一意に定義される転送コマンドを実行する。本実施例ではサーバ５からクライアント４へファイルを転送するコマンドを起動する（ステップＳ１２）。クライアント４はサーバ５より送信されるファイルを受信する（ステップＳ１３）。ファイルの送受信が完了すると、転送コマンドの動作は完了する（ステップＳ１５，Ｓ１６）。

【００２１】次に、図１，２，および本実施例のファイル転送装置をインタラクティブ方式に適用した場合の本発明の第３の実施例のファイル転送方法の処理を図３と共通の処理には共通の参照文字／数字を付して同様にフローチャートで示す図４を参照して本実施例の動作につ

いて説明すると、この図に示す本実施例のファイル転送方法と上述の第１の実施例との相違点は、ステップＳ３で確認に成功すると、サーバ５はコマンドインタプリタ５１を起動し、コマンドインタプリタ５１のプロンプトをクライアントへ表示するステップＳ５と、ユーザはクライアント４に表示されたプロンプトから転送コマンドと転送対象のファイル名とを入力するステップＳ６と、さらに、ステップＳ１２，Ｓ１３のファイル転送終了後、他に転送対象ファイルの有無を確認し無ければステップＳ１５で終了し、有ればステップＳ６へ戻り以下Ｓ１４までを反復するステップＳ１４とを付加することである。これにより、ファイル転送の度にキーワードとアクセス定義ファイルの照合が行われる。

【００２２】

【発明の効果】以上説明したように、本発明のファイル転送方法およびファイル転送装置は、キーワードと、それと組となるクライアントユーザ名，クライアントホスト名，実行コマンド，およびアクセス可能ディレクトリが予めデータベース上に定義されており、ユーザはファイル転送実行時にこのキーワードの使用を義務付けられており、クライアント毎に異なるキーワードを割当てることによって、異なるクライアント毎のアクセス可能なディレクトリの制限を可能とするという効果がある。

【図面の簡単な説明】

【図１】本発明の第１の実施例のファイル転送装置を示すブロック図である。

【図２】図１のセキュリテイ管理データベースの内容とアクセス定義データベースの内容およびアクセス範囲指＊定の一例を示す図である。

【図３】本発明の第２の実施例のファイル転送方法を示すフローチャートである。

【図４】本発明の第３の実施例のファイル転送方法を示すフローチャートである。

【図５】従来の第１のファイルファイル転送装置の一例を示すブロック図である。

【図６】従来のパスワード情報データベースの内容の例を示す図である。

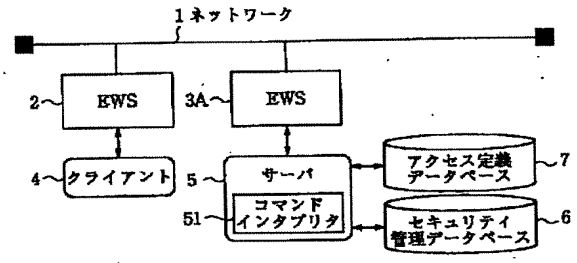
【図７】従来の第１のファイル転送方法を示すフローチャートである。

【図８】従来の第２のファイル転送方法を示すフローチャートである。

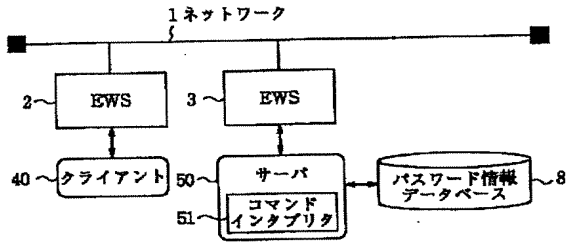
【符号の説明】

１　ネットワーク
２，３　ＥＷＳ
４，４０　クライアント
５，５０　サーバ
６　セキュリテイ管理データベース
７　アクセス定義データベース
８　パスワード情報データベース
５１　コマンドインタリプタ
６１，７１　キーワード
６２　クライアントホスト名
６３　クライアントログイン名
７２　コマンド
７３　ディレクトリ

【図１】



【図５】

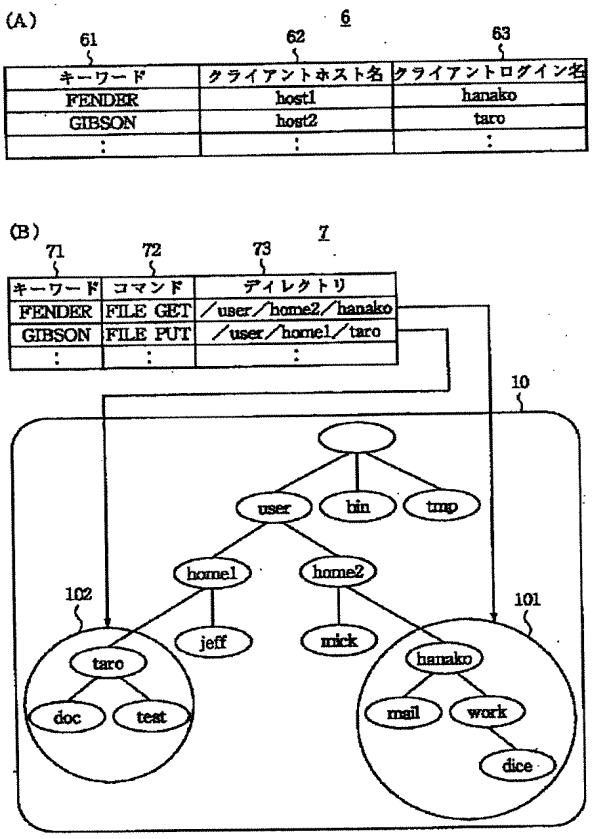


【図６】

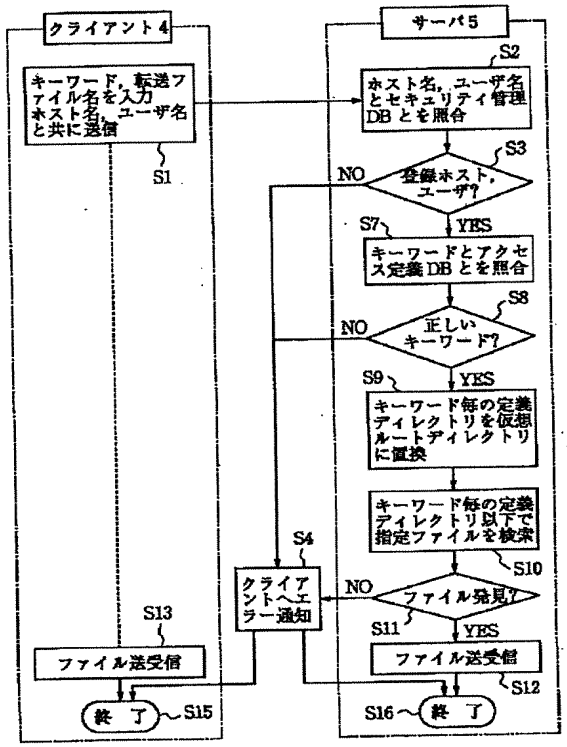
8

81 ログイン名	82 パスワード名
hanako	Pass-word
taro	sEcReTs
：	：

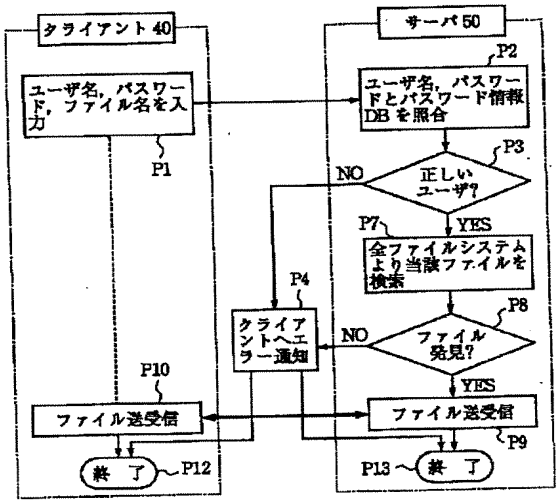
【図２】


(A)
6
61
62
63
キーワード
クライアントホスト名
クライアントログイン名
FENDER
host1
hanako
GIBSON
host2
taro
(B)
7
71
72
73
キーワード
コマンド
ディレクトリ
FENDER
FILE GET
/user/home2/hanako
GIBSON
FILE PUT
/user/home1/taro
10
user
bin
tmp
home1
home2
102
101
jeff
mick
taro
hanako
doc
test
mail
work
dice

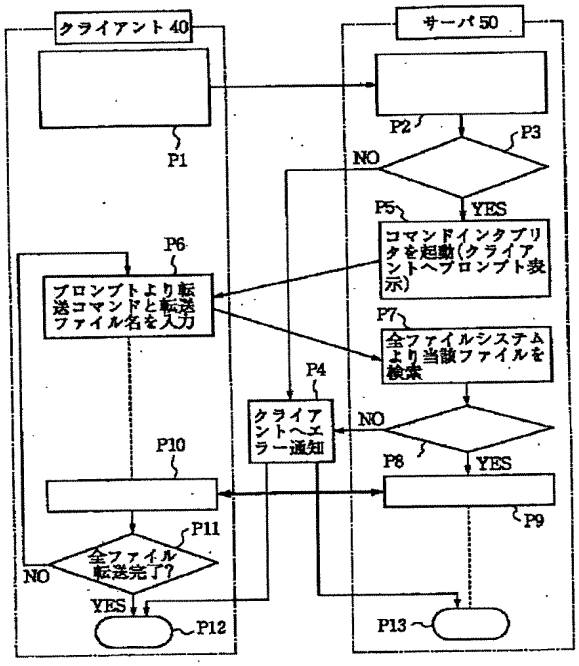
【図３】


クライアント4
サーバ5
キーワード，転送ファイル名を入力
ホスト名，ユーザ名と共に送信
S1
ホスト名，ユーザ名とセキュリティ管理DBとを照合
S2
登録ホスト，ユーザ?
S3
NO
YES
キーワードとアクセス定義DBとを照合
S7
正しいキーワード?
S8
キーワード毎の定義ディレクトリを仮想ルートディレクトリに置換
S9
キーワード毎の定義ディレクトリ以下で指定ファイルを検索
S10
ファイル発見?
S11
クライアントへエラー通知
S4
ファイル送受信
S13
ファイル送受信
S12
終了
S15
終了
S16

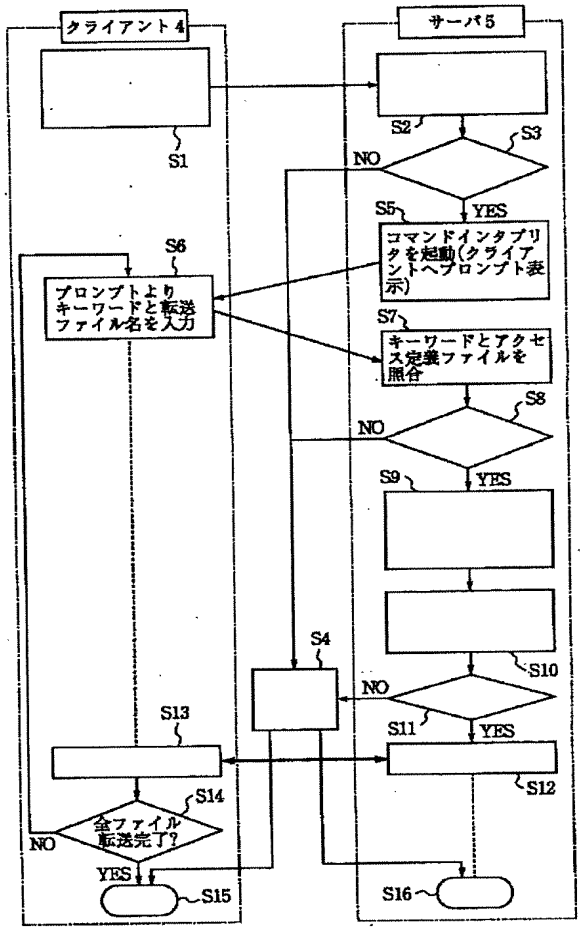
【図７】


クライアント40
サーバ50
ユーザ名，パスワード，ファイル名を入力
P1
ユーザ名，パスワードとパスワード情報DBを照合
P2
正しいユーザ?
P3
NO
YES
全ファイルシステムより当該ファイルを検索
P7
クライアントへエラー通知
P4
ファイル発見?
P8
NO
YES
ファイル送受信
P10
ファイル送受信
P9
終了
P12
終了
P13

【図８】


クライアント40
サーバ50
P1
P2
P3
NO
YES
コマンドインタプリタを起動(クライアントへプロンプト表示)
P5
プロンプトより転送コマンドと転送ファイル名を入力
P6
全ファイルシステムより当該ファイルを検索
P7
クライアントへエラー通知
P4
NO
YES
P8
P10
P9
全ファイル転送完了?
P11
NO
YES
P12
P13

【図４】


クライアント4
サーバ5
S1
S2
S3
NO
YES
S5
コマンドインタプリタを起動(クライアントへプロンプト表示)
S6
プロンプトよりキーワードと転送ファイル名を入力
S7
キーワードとアクセス定義ファイルを照合
S8
NO
YES
S9
S4
S10
NO
S11
YES
S13
S12
S14
全ファイル転送完了?
NO
YES
S15
S16